IN THE CLAIMS

No claims have been amended. Claims are reproduced below for ease of examination.

1. (Original) An apparatus comprising:

a cryptographic processor within a wireless device, the cryptographic processor comprising:

at least one cryptographic unit;

a nonvolatile memory to store one or more microcode instructions, wherein at least one of the one or more microcode instructions is related to a sensitive operation; and

a controller to control execution of the one or more microcode instructions by the at least one cryptographic unit, wherein the controller is to preclude execution of the sensitive operation if the apparatus is within an untrusted state.

2. (Original) The apparatus of claim 1, further comprising:
a volatile memory to store a cache of at least one cryptographic key and a counter, and
at least one platform configuration register.

3. (Original) The apparatus of claim 2, wherein a sensitive operation is an operation that uses a root encryption key for the apparatus, an operation that uses one of the at least one encryption key or an operation that is to access the counter or the at least one platform configuration register.

4. (Original) The apparatus of claim 2, wherein the apparatus is within the untrusted state if the apparatus is improperly initialized, if an authentication operation of one of the at least one cryptographic key fails or if one of the cryptographic units is to perform an illegal operation.

5. (Original) The apparatus of claim 4, wherein an illegal operation includes an out-of-order execution by one of the at least one cryptographic units.

6. (Original) A method comprising:

receiving a primitive instruction into a cryptographic processor within a wireless device;

retrieving at least one microcode instruction from a nonvolatile memory within the cryptographic processor based on the primitive instruction; and

executing the at least one microcode instruction if the microcode instruction is not a sensitive operation or if the at least one microcode instruction is a sensitive operation and the cryptographic processor is in a trusted state.

7. (Original) The method of claim 6, wherein executing the at least one microcode instruction if the microcode instruction is not the sensitive operation comprises executing the at least one microcode instruction if the microcode instruction does not uses a root encryption key of the cryptographic processor.

8. (Original) The method of claim 6, wherein executing the at least one microcode instruction if the microcode instruction is not the sensitive operation comprises executing the at least one microcode instruction if the microcode instruction does not uses an encryption key protected within the cryptographic processor.

9. (Original) The method of claim 6, wherein executing the at least one microcode instruction if the microcode instruction is not the sensitive operation comprises executing the at least one microcode instruction if the microcode instruction does not access a monotonic counter or data in a platform configuration register.

10. (Original) The method of claim 6 further comprising initializing the cryptographic processor prior to receiving the primitive instruction, wherein initializing comprises verifying at least one functional unit in the cryptographic processor is generating proper results.

11. (Original) The method of claim 10, wherein verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying a hash unit in the cryptographic processor is generating correct hashes.

12. (Original) The method of claim 10, wherein verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying a random number generator unit is generating random numbers.

13. (Original) The method of claim 10, wherein verifying the at least one functional unit in the cryptographic processor is generating proper results comprises verifying an exponential arithmetic unit or an arithmetic logic unit is computing proper results.

14. (Original) A method comprising:

receiving a patch of at least one microcode instruction stored in nonvolatile memory within a cryptographic processor in a wireless device; and

validating the patch during a boot operation of the wireless device prior to execution of the patch of the at least one microcode instruction, wherein the validating comprises:

validating a cryptographic key of the patch based on a hash of the cryptographic key that is stored in a one time programmable storage in a nonvolatile memory that is external to the cryptographic processor.

15. (Original) The method of claim 14 further comprising receiving a signature of the patch, wherein the validating of the patch comprises:

generating a digest of the patch using a hash unit within the cryptographic processor;

decrypting the received signature of the patch to generate a decrypted received signature;

comparing the decrypted received signature to the generated digest; and

validating the patch if the decrypted received signature equals the generated digest.

16. (Original) The method of claim 14, wherein receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving the patch from a nonvolatile memory external to the cryptographic processor.

17. (Original) The method of claim 14, wherein receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving a patch of a part of the microcode instructions in the nonvolatile memory, wherein the patch includes at least one patch flag that identifies the part of the microcode instructions to be patched.

18. (Original) The method of claim 14 further comprising loading a segment of the patch into a volatile memory within the cryptographic processor after at least one microcode instruction within the segment is to be executed in place of a microcode instruction stored in the nonvolatile memory within the cryptographic processor.

19. (Original) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving a primitive instruction into a cryptographic processor within a wireless device;

retrieving at least one microcode instruction from a nonvolatile memory within the cryptographic processor based on the primitive instruction; and

executing the at least one microcode instruction if the microcode instruction is not a sensitive operation or if the at least one microcode instruction is a sensitive operation and the cryptographic processor is in a trusted state.

20. (Original) The machine-readable medium of claim 19, wherein executing the at least one microcode instruction if the microcode instruction is a sensitive operation comprises executing the at least one microcode instruction if the microcode instruction uses a root encryption key of the cryptographic processor.

21. (Original) The machine-readable medium of claim 19, wherein executing the at least one microcode instruction if the microcode instruction is a sensitive operation comprises executing the at least one microcode instruction if the microcode instruction uses a data encryption key protected within the cryptographic processor.

22. (Original) The machine-readable medium of claim 19 further comprising initializing the cryptographic processor prior to receiving the primitive instruction, wherein initializing comprises verifying at least one functional unit in the cryptographic processor is generating proper results.

23. (Original) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving a patch of at least one microcode instruction stored in nonvolatile memory within a cryptographic processor in a wireless device; and

validating the patch during a boot operation of the wireless device prior to execution of the patch of the at least one microcode instruction, wherein the validating comprises:

validating a cryptographic key of the patch based on a hash of the cryptographic key that is stored in a one time programmable storage in a nonvolatile memory that is external to the cryptographic processor.

24. (Original) The machine-readable medium of claim 23 further comprising receiving a signature of the patch, wherein the validating of the patch comprises:
generating a signature of the patch using a hash unit within the cryptographic processor;
comparing the received signature to the generated signature; and
validating the patch if the received signature equals the generated signature.

25. (Original) The machine-readable medium of claim 23, wherein receiving the patch of the at least one microcode instruction stored in the nonvolatile memory within the cryptographic processor in the wireless device comprises receiving the patch from a nonvolatile memory external to the cryptographic processor.

26. (Original) The machine-readable medium of claim 23 further comprising loading a segment of the patch into a volatile memory within the cryptographic processor after at least one microcode instruction within the segment is to be executed in place of a microcode instruction stored in the nonvolatile memory within the cryptographic processor.

27. (Original) A system comprising:

a FLASH memory to store a hash in a one time programmable storage, wherein the hash is of a cryptographic key associated with a patch of the at least one microcode instruction; and

a cryptographic processor comprising:

a nonvolatile memory to store the at least one microcode instruction to be patched;

a number of cryptographic units; and

a controller to cause at least one of the number of cryptographic units to validate the patch based on the cryptographic key and the hash of the cryptographic key.

28. (Original) The system of claim 27, wherein the FLASH memory is to store a signature of the patch based on the cryptographic key, wherein the controller is to cause at least one of the number of cryptographic units to validate the patch based on the signature.

29. (Original) The system of claim 27, wherein the nonvolatile memory is a read only memory.

30. (Original) The system of claim 27, wherein the cryptographic processor further comprises a volatile memory, wherein the controller is to cause the patch to be loaded into the volatile memory after the patch is validated.

31. (Original) The system of claim 30, further comprising an application processor to generate a primitive instruction related to a cryptographic operation, wherein the controller is to retrieve the at least one microcode instruction related to the primitive instruction from the patch loaded into the volatile memory or from the nonvolatile memory.

32. (Original) The system of claim 31, further comprising a shared volatile memory, wherein the shared volatile memory is partitioned into a public section and a private section, wherein the public section is accessible by the cryptographic processor and the application processor, and wherein the private section is accessible by the cryptographic processor and not the application processor.